BULL. AUSTRAL. MATH. SOC. MOS 16A44
VOL. 5 (1971), 271-274.

Rings with a few more zero-divisors

C. Christensen

It is well-known that every finite ring with non-zero-divisors has order not exceeding the square of the order n of its left zero-divisor set. Unital rings whose order is precisely n^2 have been described already. Here we discuss finite rings with relatively larger zero-divisor sets, namely those of order greater than $n^{3/2}$. This is achieved by describing the class of all finite rings with left composition length two at most, and using a theorem relating the left composition length of a finite ring to the size of its left zero-divisor set.

It is known from the work of Ganesan ([2], [3]) and Koh [4] that a finite ring is either a field or its order is bounded above by n^2 where n is the number of left zero-divisors of the ring. The class of unital rings where this bound is attained has been fully described by Corbas [1]; we refer to such rings as *Corbas rings*. In the present article we describe the class of all rings with left composition length at most two and show that it contains all rings of order greater than $n^{3/2}$. In fact, given a finite ring, we give a bound on its left composition length in terms of the size of its left zero-divisor set.

Throughout, R denotes a finite ring and the set of left zero-divisors of R is denoted by λR. To avoid ambiguity: an element r of R is in λR if and only if R has a non-zero element s such that $rs = 0$. As usual, given a finite set X, the symbol $|X|$ denotes the number of elements in X. Clearly, for any element r of R, the property $|rS| < |S|$ for some subset S of R implies $r \in \lambda R$. [In

Received 7 May 1971.

particular therefore $\lambda R = \{r \mid r \in R \wedge rR \neq R\} = \bigcup\{I \mid I$ is a proper right ideal of $R\}$.] Thus if L/M is a composition factor of R considered as an R-module in the natural way, then the annihilator of L/M in R is a subset of λR . Let $x \in L-M$; then the kernel, $\ker\theta$, of the R-module homomorphism $\theta : R \to L/M$ given by $\theta : r \mapsto rx+M$ for all $r \in R$ annihilates L/M and hence lies in λR . It follows that $|R| \leq |L/M||\ker\theta| \leq |L/M||\lambda R|$ so that $|L/M| \geq |R||\lambda R|^{-1}$. From this one deduces immediately:-

THEOREM 1. *Let* $|\lambda R| \leq |R|^{1-\varepsilon}$ *where* ε *is a positive real number less than* 1 ; *then every left composition factor of* R *has order no less than* $|R|^{\varepsilon}$ *and hence the left composition length of* R *is at most* $\frac{1}{\varepsilon}$.

In particular, therefore, the class of finite rings R such that $|\lambda R| < |R|^{2/3}$ is contained in the class whose left composition length is at most two. We describe the latter class in the next theorem.

THEOREM 2. *The left composition length of* R *is at most two if and only if* R *is one of the following types:-*

(i) *a field;*

(ii) *a ring direct sum of two fields;*

(iii) *a complete ring of* 2×2 *matrices over a field;*

(iv) *a ring direct sum of a field and a null ring of prime order;*

(v) *a ring direct sum of two null rings of prime orders;*

(vi) *a null ring with additive group of order* p *or* p^2 *where* p *is a prime;*

(vii) $\langle a, b \mid pa = pb = 0 \wedge a^2 = b \wedge a^3 = 0\rangle$ *where* p *is a prime;*

(viii) $\langle a \mid p^2a = 0 \wedge a^2 = pa\rangle$ *where* p *is a prime;*

(ix) $\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in K\right\}$ *where* K *is a field;*

(x) $\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in K\right\}$ *where* K *is a prime field;*

(xi) *a Corbas ring.*

https://doi.org/10.1017/S0004972700047158 Published online by Cambridge University Press

Proof. That all rings of types *(i)* to *(xi)* have left composition length at most two is clear.

Conversely, let R have left composition length at most two. Then if R is semisimple it is of type *(i)*, *(ii)* or *(iii)*. If R is decomposable into a direct sum of two proper ideals, it is of type *(ii)*, *(iv)* or *(v)*. If R is nilpotent and not directly decomposable then it is of type *(vi)* or $R^2 \neq \{0\}$. For the latter case it is clear that $R > R^2 > R^3 = \{0\}$ is a left composition series for R and it follows that the null rings R^2 and R/R^2 have no proper left ideals; consequently their additive groups are cyclic of prime order. Because R is directly indecomposable it has prime power order and therefore $|R| = p^2$ for some prime p. If the additive group R^+ of R is elementary abelian then let a and c generate R^+ and choose $c \in R^2$. Then $a^2 = kc$ for some positive integer k where $p \nmid k$. Since $b = kc$ also generates R^2, R is of type *(vii)*. If, on the other hand, R^+ is cyclic, let b be one of its generators. Then b has order p^2 and since $b^2 \in R^2$ which is non-zero and has order p, it follows that $b^2 = pkb$ for some positive integer k coprime with p. Let m be a positive integer such that $mk \equiv 1 \pmod{p}$, then $a = mb$ also generates R^+ and $a^2 = pa$ so that R is of type *(viii)*.

It remains only to consider non-nilpotent, non-semisimple rings that are not directly decomposable. Let J be the Jacobson radical of such a ring, then R/J is a field and $J^2 = \{0\}$ since R has left composition length two. The condition $J^2 = \{0\}$ allows us to define the multiplication $(r+J)j = rj$ for all $r+J \in R/J$ and $j \in J$. If R is unital, then J is a one-dimensional vector space over R/J under this operation and hence $|J| = |R/J|$; it is now easy to check that $\lambda R = J$ so that $|R| = |\lambda R|^2$ and R is a Corbas ring. Consider therefore the non-unital case. Let $e + J$ be the identity of R/J, then

$$(3e^2-2e^3)^2 - (3e^2-2e^3) = 4(e^2-e)^3 - 3(e^2-e)^2 \in J^2 = \{0\}$$

so that as usual $3e^2 - 2e^3$ is an idempotent congruent to e mod J. Without loss of generality assume that e is itself idempotent. Since $e + J$ is the identity of R/J, the sets $\{r-re \mid r \in R\}$ and $\{r-er \mid r \in R\}$ are both contained in J and as we have assumed that R is non-unital, at least one of them is not $\{0\}$. The first set is a left

https://doi.org/10.1017/S0004972700047158 Published online by Cambridge University Press

ideal and therefore is $\{0\}$ or J. The latter implies that $R = Re \oplus J$ and that $Je = \{0\}$. Moreover Re is then a field $(\cong R/J)$ with identity e in which case $JR = JRe = \{0\}$. Since by assumption R is not directly decomposable as a ring, Re is not an ideal so that $eJ \neq \{0\}$ and as a left Re-module J is a 1-dimensional vector space. Therefore in this case R is of type *(ix)*. It remains only to consider the case

$$\{r-re \mid r \in R\} = \{0\} \neq \{r-er \mid r \in R\} .$$

Thus e is a right identity in R and $\{r-er \mid r \in R\}$ is a left ideal contained in and therefore equal to J. Hence $R = J \oplus eR$, $eR \cong R/J$ is a field and J is unital as a right eR-module; moreover, as $RJ = J^2 + eRJ = eJ = \{0\}$ and J is a minimal left ideal, $|J|$ must be a prime. It follows that R is of type *(x)*.

It is a simple matter to deduce the following result from the preceding theorems.

COROLLARY. $|\lambda R|^{3/2} < |R|$ *if and only if* R *is of type (i), of type (ii) with the order* a, b *of the fields satisfying* $a^2b^2 - (a+b-1)^3 > 0$, *of type (ix) or of type (xi). The rings of types (ix) and (xi) are those where* $|\lambda R|^2 = |R|$.

References

[1] Basil Corbas, "Rings with few zero divisors", *Math. Ann.* 181 (1969), 1-7.

[2] N. Ganesan, "Properties of rings with a finite number of zero divisors", *Math. Ann.* 157 (1964), 215-218.

[3] N. Ganesan, "Properties of rings with a finite number of zero divisors II", *Math. Ann.* 161 (1965), 241-246.

[4] Kwangil Koh, "On 'Properties of rings with a finite number of zero divisors'", *Math. Ann.* 171 (1967), 79-80.

Department of Pure Mathematics,
School of General Studies,
Australian National University,
Canberra, ACT.